ABSTRACT

[1099] Techniques for efficient KASUMI ciphering are disclosed. In one aspect, one KASUMI round for generating a fractional portion of the KASUMI cipher is deployed with appropriate feedback such that eight sequential rounds produce the KASUMI output. In another aspect, one third of the FO function is deployed with appropriate feedback such that three successive cycles produce the FO output. In yet another aspect, the FI function is deployed with appropriate feedback such that two subsequent cycles produce the FI output. In yet another aspect, a sub-key generator comprising two shift registers produces sub-keys for each round and sub-stage thereof in an efficient manner. These aspects, collectively, yield the advanced benefits of low area and low cost implementations of KASUMI with a simple user interface. Various other aspects of the invention are also presented.